

Praktikumsversuch 3: Public-Key-Verschlüsselung

Datenbanken und Datensicherheit · Wintersemester 2024/25 · Prof. Dr. Peter Gerwinski

Aufgabe: Tauschen Sie mit einem Betreuer – unter Berücksichtigung aller Sicherheitsmaßnahmen beim Schlüsselaustausch – verschlüsselte E-Mails gemäß dem OpenPGP-Standard aus.

- Installieren Sie auf einem Rechner Software eigener Wahl zum Versenden und Empfangen von verschlüsselter E-Mail gemäß dem OpenPGP-Standard (RFC 4880/5581/6637). Geeignete Software finden Sie per Web-Suche.
- Erstellen Sie für sich selbst ein Schlüsselpaar, bestehend aus einem öffentlichen und einem geheimen Schlüssel.
- Lassen Sie Ihnen öffentlichen Schlüssel einem Betreuer zukommen. Stellen Sie durch Vergleich der Schlüssel-Fingerabdrücke sicher, daß der Schlüsselaustausch erfolgreich war.
- Besorgen Sie sich den öffentlichen Schlüssel eines Betreuers. Stellen Sie durch Vergleich der Schlüssel-Fingerabdrücke sicher, daß der Schlüsselaustausch erfolgreich war.
- Senden Sie eine verschlüsselte Nachricht an einen Betreuer. Sobald Sie darauf eine verschlüsselte Antwort bekommen und entschlüsseln können, ist der Praktikumsversuch bestanden.
- Optional: Überzeugen Sie Ihren Betreuer von Ihrer persönlichen Identität (z. B. durch Vorzeigen eines amtlichen Lichtbildausweises) und lassen Sie sich von ihm Ihren persönlichen öffentlichen Schlüssel unterschreiben (zertifizieren).
- Optional: Überzeugen Sie sich von der persönlichen Identität Ihres Betreuers, unterschreiben (zertifizieren) Sie seinen öffentlichen Schlüssel und lassen Sie ihm seinen eigenen Schlüssel mit Ihrer Unterschrift zukommen.
- Hintergrund: Durch das gegenseitige Zertifizieren von Schlüsseln entsteht ein *Web of Trust*.

Viel Erfolg!

Stand: 8. Januar 2025

Copyright © 2024, 2025 Peter Gerwinski

Lizenz: CC BY-SA (Version 4.0) oder GNU GPL (Version 3 oder höher)

Sie können diese Praktikumsunterlagen einschließlich \LaTeX -Quelltext herunterladen unter:

<https://gitlab.cvh-server.de/pgerwinski/dbs>